FORTINET TRAINING SERVICES

Feature Overview – Func Specs

- In 5.0 and before, when adding a new policy, we need to specify whether it is address based, user identity based or device identity based.
- In 5.2, it is better that the policy type is figured out automatically by FOS. This means we allow user to put any combination of the following into source address object
  - » user or user group
  - » device or device group
- The default implicit for user ID or device ID based policy should be fall-through.

FORTINET

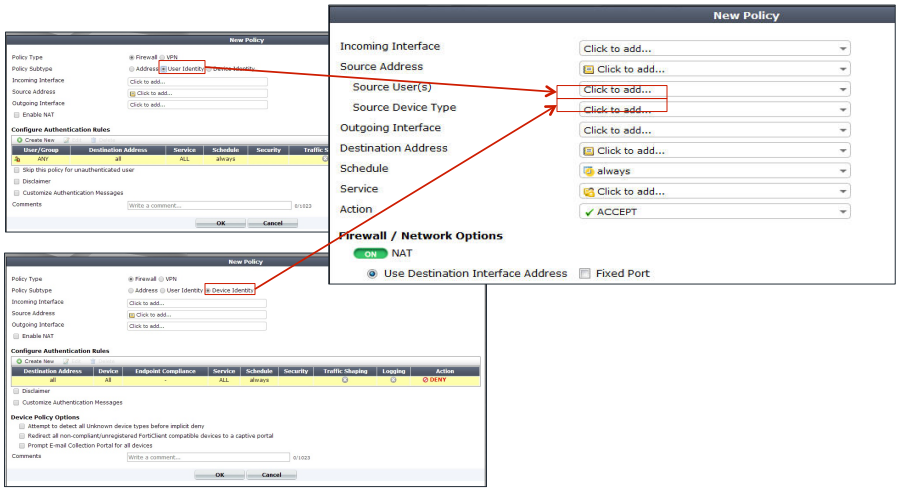
Feature Overview – Motivation

- The motivation behind this change came from a Feature request

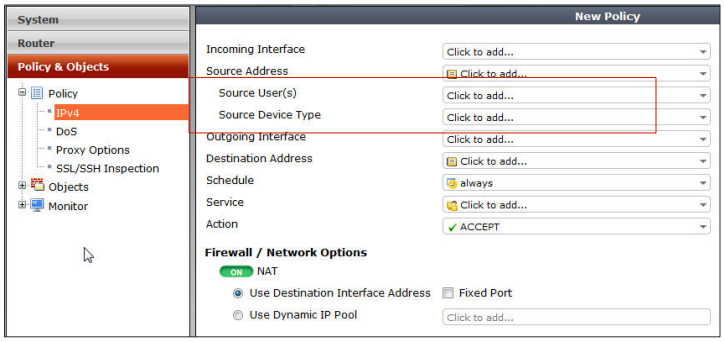
"This is a strong competitive criteria against PAN, Checkpoint, Cisco, all of which incorporate identity at the main policy level, rather than within a sub policy. Such a policy engine is easier to work with for the vast majority of customers."

"Customer feedback on our identity policy engine is that it is complex and not flexible enough. Customer feedback on device policies is that they are unusable if they cannot be combined with identity policies - their current use case is limited to wireless BYOD deployments."

Changes – GUI Comparison



Changes – Policy integration



- User and Device ID are merged into 1 single flat configuration
- This enables user to select both user groups and device groups in the same policy

Changes - Default Implicit Fall-through

- In 5.2, by default there is an *implicit* fall-through enabled on each authentication policy
- traffic will fall-through to the next policy:
  1. Traffic had not been previously authenticated OR traffic had been authenticated but it doesn't match the user/group within the current policy
  2. There is another policy below the current one that also matches the src/dst/service of the traffic
- There is no option to disable this behaviour
- The option "fall-through-unauthenticated" from 5.0 is removed

Changes – Example 1

Example 1 for 5.2:

- There are 2 policies from internal->wan1
- Policy 1: user=group1, service=all, action=accept
- Policy 2: user=none, service=all, action=accept

- When an unauthenticated user tries to go through, FortiGate first tries to match policy 1.
- However, because user is unauthenticated, AND there is another policy behind it that also matches, it will fall-through to the next policy
- **Result:** traffic matches policy 2 and user never receives an authentication prompt

7 FORTINET

Changes – Example 2

Example 2 for 5.2:

- There is 1 policy from internal->wan1
- Policy 1: user=group1, service=all, action=accept

- Suppose in this example, there is only 1 policy.
- When an unauthenticated user tries to go through, FortiGate first tries to match policy 1
- Since the user is unauthenticated, AND there is no other policy behind this, the FortiGate will match this policy and display an authentication page
- **Result:** No fall-through. User is prompted to authenticate

8 FORTINET

Changes – 5.0 behavior

- In **5.0**, without “fall-through-unauthenticated” enabled, the results of the 2 examples would be as follows

Example 1:

- An unauthenticated user matching the src/dst/port of policy 1 will be prompted for authentication. Auth success/failure will determine the action

Example 2:

- Same result as Example 1

9

FORTINET

Changes – Comparison with “fall-through-unauthenticated”

- The option “fall-through-unauthenticated” was added in 5.0.1 to allow unauthenticated users to fall-through to the next policy
- This solved the problem of unauthenticated users getting “stuck” in an identity policy that didn’t match its user group
- However, this only allowed unauthenticated users to fall-through, not users that were already authenticated but didn’t match the group(s) within the ID policy

```
config firewall policy
    edit 1
        set srcintf "port1"
        set dstintf "port2"
        set srcaddr "all"
        set action accept
        set fall-through-unauthenticated
enable
        set identity-based enable
.....
```

10

FORTINET

Changes – Example 3

Example 3:

- suppose a customer has 2 user groups A & B from the same network segment that needs to pass through the FortiGate
- The only difference is that each group needs to nat'd with a different IP
- To accommodate this, 2 rules are created:

RULE 1:
SRC IP is the Subnet of GroupA and B
SRCZone is "LAN"
DSTZone is "WAN"
NAT – Hide Nat with IP A
Sub Authentication Rule
Group: Group A
Dst Any
Service Any
Action: allow

RULE 2:
SRC IP is the Subnet of GroupA and B
SRCZone is "LAN"
DSTZone is "WAN"
NAT – Hide Nat with IP B
Sub Authentication Rule
Group: Group B
Dst Any
Service Any
Action: allow

11

Changes – Comparison with "fall-through-unauthenticated"

- In 5.0, with one rule behind the other, a user that is authenticated will always hit Rule 1.
- Hence, for users in Group B, it will always be denied access because the policy match always end at Rule 1
- The "fall-through-unauthenticated" option only applies to unauthenticated users
- In 5.2 however, this same configuration will work because the implicit fall-through applies to all authenticated and unauthenticated users
- If the authenticated user doesn't match the group, it will move on to the next policy

12

Changes – valid Authentication protocols

- In 5.0, supported authentication protocols are http/https/ftp/ telnet
- These are all supported methods no matter if the authentication policy allows these services or not
- In 5.2 authentication protocols can be used only if it is an allowed service within the authentication policy

- Example:
- There is 1 policy from internal->wan1
- Policy 1: user=group1, service=PING, action=accept
  - » With 5.0 http/https/ftp/telnet user will receive authentication prompts
  - » With 5.2 http/https/ftp/telnet will NOT receive authentication prompts

13 FORTINET

Changes – Other authentication Caveats

DNS:

- In 5.0, DNS is implicitly supported by the authentication policy
  - » In order to successfully authenticate users will likely need to be able too resolve hostnames
  - » Even if DNS is not allowed by the Authentication policy it is allowed to pass

- In 5.2, the authentication policy must include DNS as a service in order to pass

14 FORTINET

DNS behavior with authentication: example

Scenario 1:
Users: Group A, Source: All IPs, Service: All, Destination: All

Behavior in 5.2
DNS is allowed to pass through prior to successful authentication
Behavior in 5.0
Same as 5.2

Scenario 2:
Users: Group A, Source: All IPs, Service: HTTP+DNS, Destination All

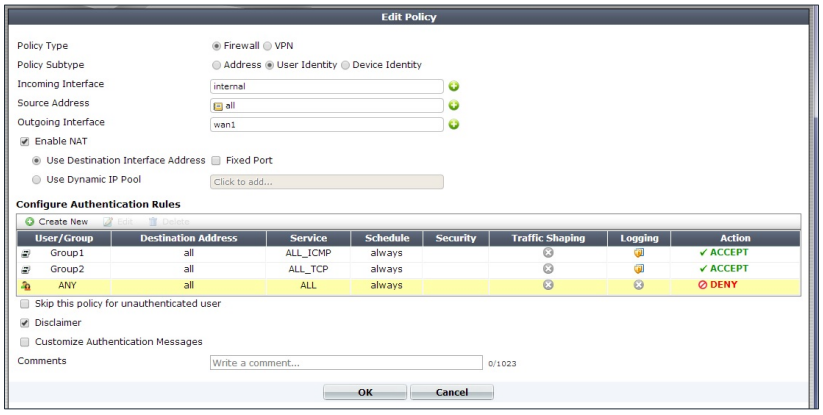
Behavior in 5.2
DNS is allowed to pass through prior to successful authentication
Behavior in 5.0
Same as 5.2

Scenario 3:
Users: Group A, Source: All IPs, Service: HTTP, Destination All

Behavior in 5.2
DNS is prevented from passing.
Behavior in 5.0
DNS is allow to pass

Upgrade Example

- Suppose you configured a User Identity-based policy with 2 Authentication Rules in 5.0.6



Upgrade Example

- Upgrade will automatically convert each authentication rule within the identity policy into its own, separate policy

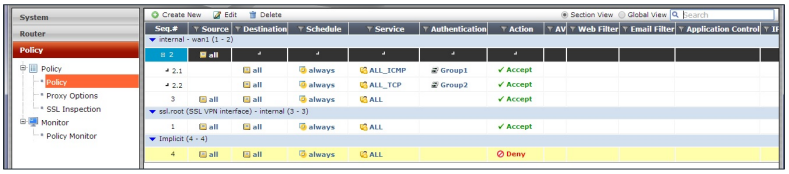
```
config firewall policy
    edit 3
        set srcintf "internal"
        set dstintf "wan1"
        set srcaddr "all"
        set action accept
        set log-unmatched-traffic enable
        set disclaimer enable
        set identity-based enable
        set nat enable
            config identity-based-policy
                edit 1
                    set schedule "always"
                    set groups "Group1"
                    set dstaddr "all"
                    set service "ALL_ICMP"
                next
                edit 2
                    set schedule "always"
                    set groups "Group2"
                    set dstaddr "all"
                    set service "ALL_TCP"
                next
            end
    next
end
```

```
config firewall policy
    edit 3
        set srcintf "internal"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL_ICMP"
        set groups "Group1"
        set disclaimer enable
        set nat enable
    next
    edit 5
        set srcintf "internal"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL_TCP"
        set groups "Group2"
        set disclaimer enable
        set nat enable
    next
```

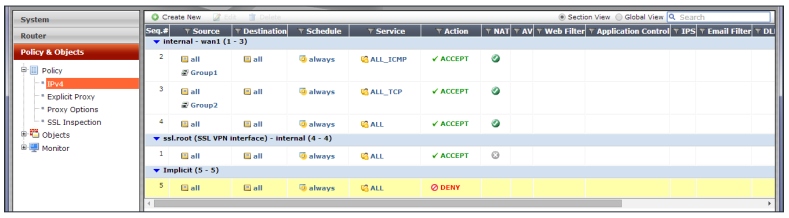
17

Upgrade Example

- Firewall Policy view in 5.0.6



- After Upgrading to 5.2.0



18

Upgrade Example: Behavior in 5.2

- When the identity of the end-users is unknown (or they are not in group1 or group2), they fall-through policy 2 and 3 as they don't match
- When they hit policy 4 users will be allowed to access the internet without prompting for their identity.
- Workaround: Disable or remove policy 4. Traffic will then match policy 3, and prompt the user for authentication

Pre-Upgrade checks

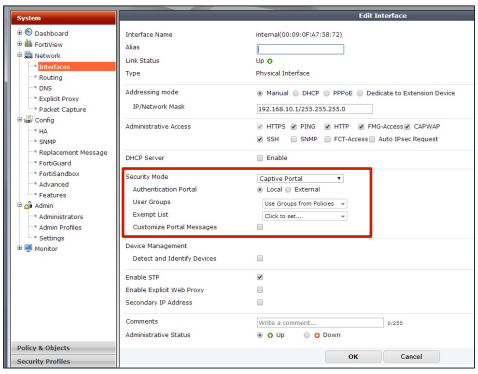
- Since the default behaviour in 5.2 has changed, it is important to take precautions before upgrading
- Check:
  1. How are the current firewall polices constructed?
  2. Which identity policies use "fall-through-unauthenticated" and which do not?
  3. Are there open-ended allow-all or deny-all policies behind the last identity-based policy? Do these need to be there?
  4. How will behaviour change if all identity polices were to become fall-through?
  5. Is the unit close to the policy limit in the max values table? Each auth rule becomes a firewall policy.

Configuration – Captive Portal

- In some scenarios, the use of Captive Portal may be a better choice
- There are 2 major steps:
  1. Enable captive portal on the ingress interface
  2. Configure the firewall policy with the appropriate User or Device groups

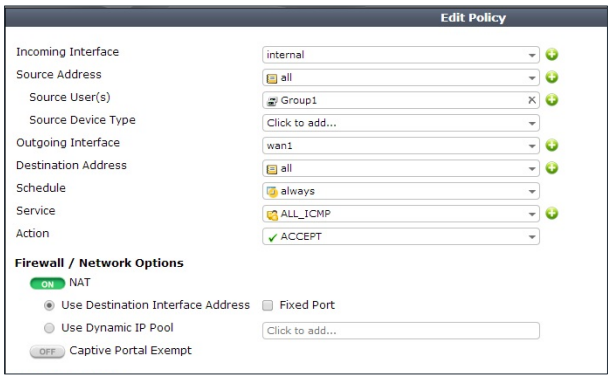
Configuration – Step 1: Enable Captive Portal

- Suppose I want to authenticate users behind the internal interface, going to the internet via wan1
- First, enable the Captive Portal on internal interface



Configuration – Step 2: Configure the ID policy

- Configure the firewall policy with Source User(s) and/or Source Device Type



Configuration – Step 3: Properly position the policy

- Move the policy to the desired position

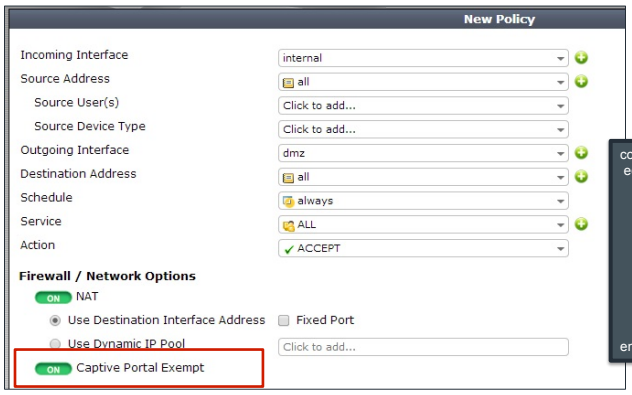
Captive Portal Exempt

- Since the captive portal is enabled on the interface, that means **any** firewall policy with that ingress interface will trigger authentication
- In some scenarios, that might not be the desired outcome
- For example, the customer might wish to authenticate all internal->wan1 traffic, but might not need to authenticate internal->dmz traffic
- Users must enable captive-portal-exempt on the firewall policy

25

FORTINET

Captive Portal Exempt

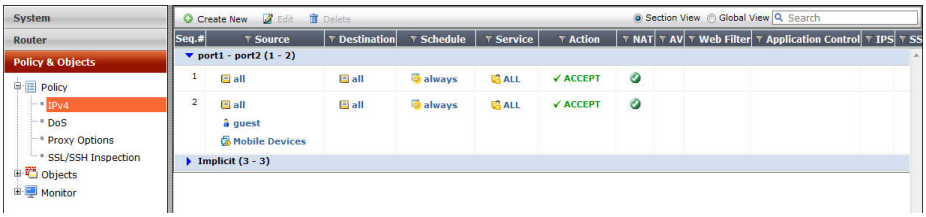


- This suppresses the Captive Portal from appearing, on this firewall policy

26

FORTINET

Captive Portal Exempt

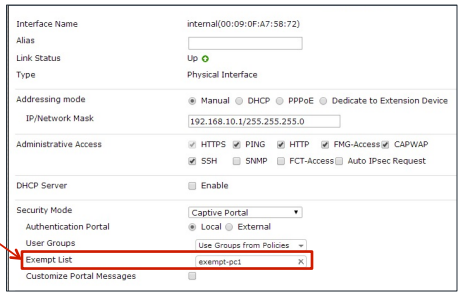


- In this scenario, traffic from internal->dmz is exempt from the Captive Portal, but traffic from internal->wan1 will require authentication via Captive Portal

Security Exempt Lists

- When the deployment has multiple egress interfaces, having to bypass Firewall policies with Captive portal exempt could become tedious to configure and maintain
- Alternatively, Security exemption list can be created in CLI
  - » After creation can be enabled on ingress interface from GUI or CLI

```
config user security-exempt-list
    edit "exempt-pc1"
        config rule
            edit 1
                set srcaddr "192.168.10.169"
            next
        end
    next
end
```



Additional Caveats

- In 5.0, the disclaimer option can be configured on the policy to display a disclaimer before authentication takes place
- In 5.2, with authentication taken out and put into the interface Captive Portal, the disclaimer does not display properly when Captive Portal is enabled
- Also, with disclaimer enabled, it always prompts for the Captive Portal, even when captive-portal-exempt is enabled

29

End

30